International Journal of Computer Science Engineering
and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 5, Issue 5, Oct 2015, 17-26

IMAGE ENCRYPTION AND COMPRESSION SYSTEM USING HAAR, DAUBECHIES AND COIFLET WAVELETS

JASPREET SINGH[1] & PRABHJOT KAUR[2]

[1]Assistant Professor, Department of Computer Science & Engineering, Chandigarh University, Gharuan, Punjab, India

[2]ME Student, Department of Computer Science & Engineering, Chandigarh University, Gharuan, Punjab, India

ABSTRACT

There has been lot of development in the field of multimedia and network technologies. With the development of multimedia and network technologies, the security of multimedia system becomes most important part in the internet when the data is transmitted over the network. If encryption is not performed then there may be possibility of stealing the information. Image compression is also essential where images need to be stored, transmitted or viewed quickly and efficiently. Therefore, there is need of system where encryption is done prior to the image compression. The main problem is how to execute image encryption and compression algorithms in pair. This paper proposed an image encryption method that is operated with random permutation method and image compression algorithm using Haar, Daubechies and Coiflet wavelet transforms that can be used efficiently to compress the encrypted image.

KEYWORDS: Compression, Coiflet, Daubechies, Encryption, Haar, Random Permutation

INTRODUCTION

An image is considered to be a two dimensional signal through the human visual system. The signals representing images are commonly in the analog form. For processing, storage and transmission by computer applications, it has to be exchanged from analog form to digital form. A digital image consists of two-dimensional array of pixels[1]. An image may be defined as a two-dimensional function f(x, y), where x and y are spatial coordinates and the amplitude of f at any pair of coordinates (x, y) is called the intensity or gray level of the image at that point. When x, y, and the amplitude values of f are all finite and discrete quantities, it is called as digital image[2].Image is the important part of data, mainly in remote sensing, biomedicine and video conferencing applications. The use of data depends on information and computers continue to grow, so there is need for efficient ways of storing and transmitting large amount of data [3].

Image Encryption

In today's scenario, lot of sensitive information is stored as digital data and transmitted over the internet. Thus, it becomes quite essential to ensure proper security and safety of the information. Information that needs to be protected consists of both textual data as well as images. Hence, image security/protection from unauthorized access becomes very important. Image Encryption refers to converting an image to such a format, so that it becomes unreadable to unauthorized access and can be transmitted securely over the internet. Image Decryption means to convert the unreadable format of an image to an original image [4]

Figure.1: Encryption of an Image Lena

There are various encryption techniques [5]:

- **DCT Based***:* Discrete cosine transformation (DCT) transforms data into frequency domain. Data can be designed by the arrangement of coefficients. DCT based techniques are compression oriented e.g. Zig-Zag Permutation. The main advantage of technique is that the energy of the original data is represented in low frequency components which depends on correlation in the area. The signal is represented in the form of the total sum of cosine functions that have different frequencies [6].
- **Wavelet Based***:* It is a small wave that converts a signal into a series of wavelets which provides a way for analyzing waveforms, bounded in both frequency and duration. The wavelet based techniques are also compression oriented. e.g. Coefficient Selective Bit Encryption [6].
- **Random Permutation Based:** It is type of symmetric cryptography technique that utilizes pseudo random index generator for the creation of keys. The three basic permutation techniques namely bit permutation, pixel permutation and block permutation are employed in any random order to encrypt the image [7].

Image Compression

An image compression system consists of processes leading to compact representation of an image, so as to reduce total storage/transmission requirements [8]. One or more of the three basic data redundancies has to be removed for achieving image compression are as follows:-

- **Coding Redundancy**: When more than optimum code words are used for image representation, coding redundancy is generated.
- **Inter-pixel Redundancy**: Inter relations between the pixels of an image may lead to inter-pixel redundancies.
- **Psycho-visual Redundancy**: Data pertaining to visually non essential information that is ignored by human visual system is known as Psycho-visual redundancy.

While reducing number of bits required to represent an image for compression, it is pertinent to ensure that reconstructed image after decompression must have almost same visual quality and resolution as that of the an original image. Image compression system is generally divided into two structural blocks: an encoder and a decoder. As indicated in the Fig. 2 Coding, inter-pixel and psycho-visual redundancies of input image are reduced by encoder process. Mapper converts image into a pattern designed to bring down inter-pixel redundancies. Then, accuracy of mapper's output is lowered by qunatizer block in line with the predefined criterion. Finally, a code for quantizer output is generated by symbol coder and output is generated in line with code. The opposite operations of the encoder's symbol decoder and inverse mapper. Inverse quantization is not included, as quantization is irreversible [9].

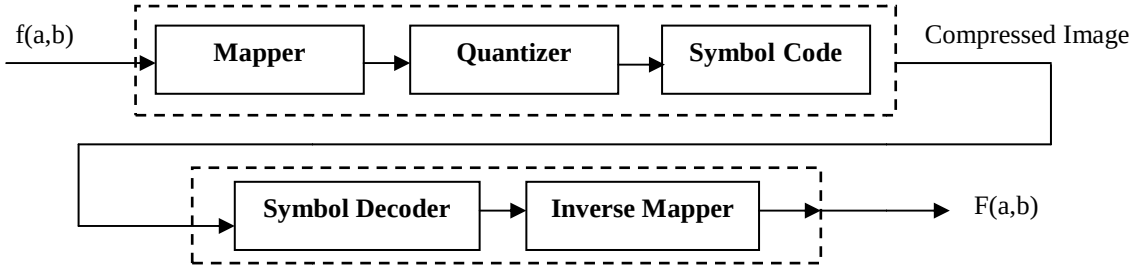

Figure 2: Block Diagram for Image Compression

Image Compression Techniques

An image compression techniques are divided into two types based on final decompressed output[10].

Table1: Comparison of Lossless and Lossy Technique

Lossless Technique	Lossy Technique
1) An original image can be perfectly recovered from the compressed (encoded) image. 2) It does not add noise to the signal (image). It is also known as entropy coding. 3) It uses statistics techniques for eliminating redundancy. 4) It is useful for a few applications with stringent requirements such as medical images. 5) Lossless schemes provide lower compression ratios than Lossless schemes. 6) It includes following techniques: 1. Run length encoding 2. Huffman encoding 3. LZW coding 4. Area coding	1) An original image cannot be perfectly recovered from the compressed (encoded) image. 2) It adds noise to the signal(image). 3) There is no use of statistics techniques to eliminate the redundancy. 4) It is widely used since the quality of the reconstructed images is adequate for most applications. 5) It provides much higher compression ratios 6) It includes following techniques:: 1. Transformation coding 2. Vector quantization 3. Fractal coding 4. Block Truncation Coding 5. Sub-band coding

The choice of wavelet function is crucial for performance an image compression. There are a number of basis that decides the choice of wavelet for image compression. The wavelet family includes the following:

Haar Wavelet: It is first and most widely used wavelet. Haar wavelet is discontinuous, and resembles a step function. The Haar Wavelet Transformation is a simple form of compression which involves averaging and differencing terms, storing detail coefficients, eliminating data and reconstructing the matrix such that the resulting matrix is similar to the initial matrix[11].

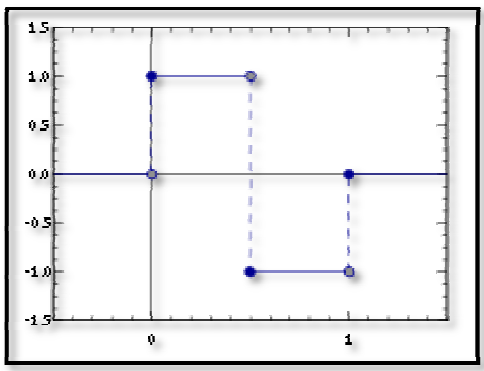

Figure 3: Haar Function on Real Line

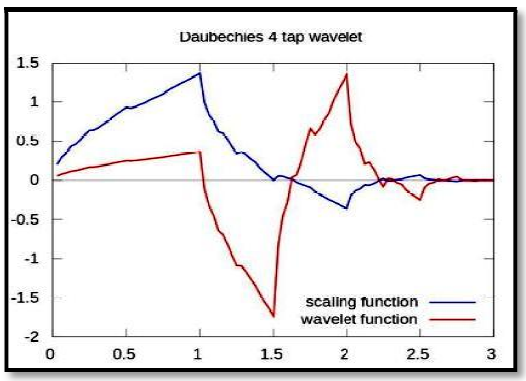

Figure 4: Daubechies Wavelet

Daubechies Wavelet*:* These are family of orthogonal wavelets defining a DWT and are characterized by a maximal number of vanishing moments for some given support. With each wavelet type of this class, there is a scaling function (called father wavelet) which generates an orthogonal multi-resolution analysis. Mainly Daubechies wavelets are chosen which have the highest number A of vanishing moments, for given support of width N=2A. There are two naming schemes: DN used for the length or number of taps, and dbA used to the number of vanishing moments. So therefore D4 and db2 are the same wavelet transform. Daubechies wavelets are used for solving the big problems e.g. self-similarity properties of a signal, fractal problems, signal discontinuities etc.[11][12]

Coiflet Wavelet*:* The wavelet function has 2N moments equal to 0 and the scaling function has 2N-1 moments equal to 0. The two functions have a support of length 6N-1. General characteristics: Compactly supported wavelets with highest number of vanishing moments for both phi and psi for a given support width[13].

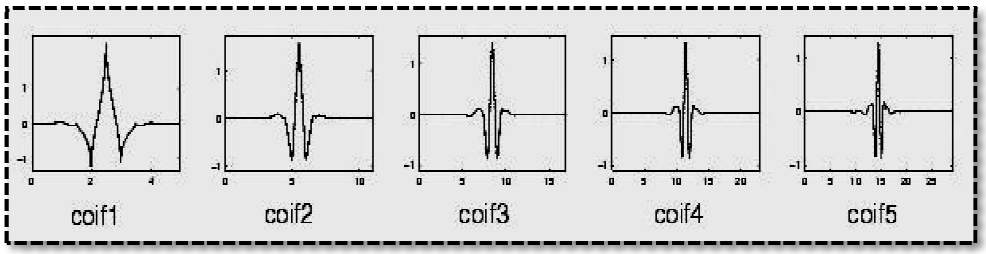

Figure 5: Coiflet Wavelet Family

Proposed Methodology

In the proposed work, image encryption is performed with random permutation method and compression by Haar, Daubechies and Coiflet wavelet transformation.The proposed approach is named as Encryption-Compression system using Haar, Daubechies and Coiflet wavelet transform [14].

As shown in figure.6, the input image is considered as 'I', encryption over 'I' is implemented using random permutation method. The result obtained after encryption is considered as 'I_e' and then Haar, Daubechies and Coiflet Wavelet technique is applied for compression. The output after compression has been stored as image 'B'. Then the image 'B' is decrypted after decompression. The resultant image $\hat{I}$ is evaluated using various performance parameters like CR, BER, MSE, PSNR, Entropy and compared with the results of an existing system. The proposed schema is also represented in the form of flowchart. Fig. 7 represents flowchart that represents the procedural flow of various steps. Half of the flowchart represents encryption steps and rest represents the compression steps.

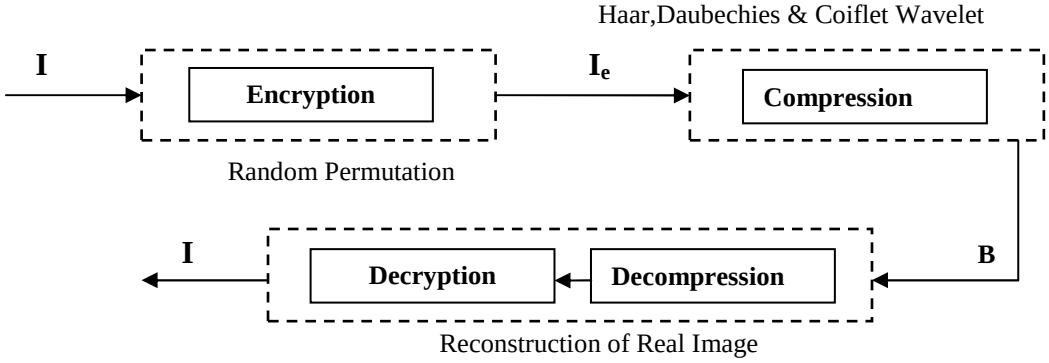

Figure 6: Proposed Model For Encryption-Compression System

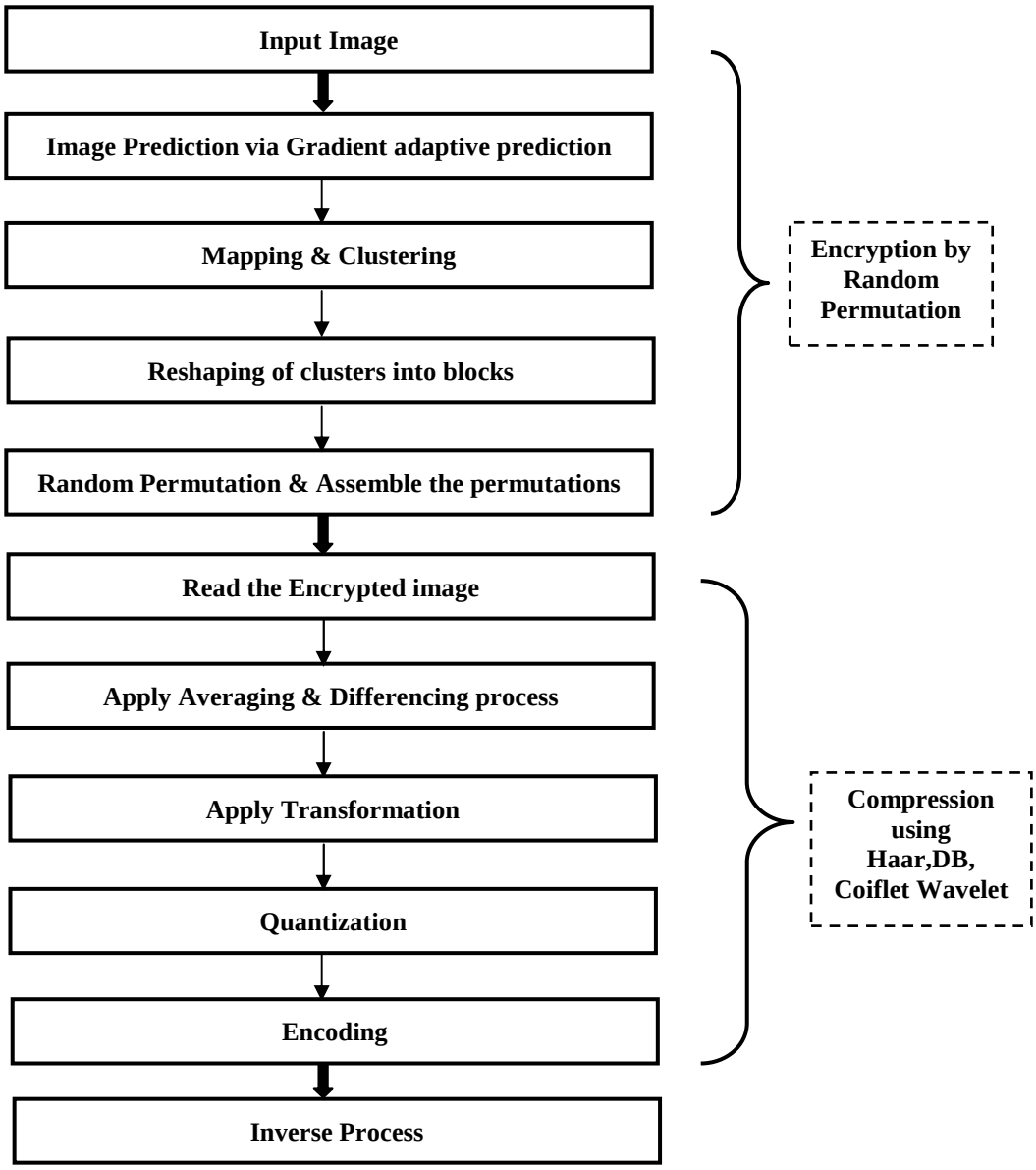

Figure 7: Flow-Chart of Image Encryption and Compression Scheme

Step 1: Implementation of Encryption Algorithm to an Input Image I

- Calculate all the mapped prediction errors $\tilde{e}_{i,\,j}$ through the real image I using Gradient adaptive prediction (GAP) image predictor.
- Divide all the prediction errors into L clusters C_k, for $0 \leq k \leq L - 1$ and concatenate the mapped prediction errors in a raster-scan order then each C_k is generated.
- 2-D block contains four columns in which reshape the prediction errors in each C_k $\lceil |C_k|/4 \rceil$ rows, where $|C_k|$ denotes the number of prediction errors in C_k.
- Applying the cyclical shift operations to each prediction error block and get the data through the raster-scan order to generate the permuted cluster $\tilde{C}_k$.

- The assembler integrate all the permuted clusters $\tilde{C}_k$, for $0 \leq k \leq L-1$ and form the resultant encrypted image $I_e=\tilde{C}_0\tilde{C}_1\ldots\tilde{C}_{L-1}$ in which each prediction error is represented by 8 bits.The number of prediction errors is equal to that of the pixels, the file size before and after the encryption preserves.
- Pass I_e together with the length of each cluster $|\tilde{C}_k|$, for $0 \leq k \leq L-2$.

Step 2: Implementation of Compression Algorithm to the Outcome of above Algorithm i.e. I_e.

- Treat the array as $\frac{n}{2}$ pairs called (a, b).
- Calculate $\frac{a+b}{\sqrt{2}}$ for each pair, these values will represent the first half of the output array.
- Calculate $\frac{a-b}{\sqrt{2}}$ for each pair, it will represent the second half.
- Repeat the process on the first half of the array (the array length should be a power of two).
- The proposed sparse orthogonal transform matrix can be obtained by appropriately inserting some 0's and $\frac{1}{2}$'s into the HWT.
- Take first four entries as two pairs then take their averages. The third and the fourth entries are obtained by subtracting these averages from the first element of each pair by multiplying the matrix on right.

Step 3: Applying the Inverse Process for Decompression & Decryption

- Calculate the inverse of all the intermediate matrices and multiply them.
- Real image will be retrieved by the resultant matrix.

Step 4: Performance Evaluation of the Reconstructed Image

Calculate Compression ratio (CR), Bit Error rate (BER), Mean-Square Error (MSE), Peak Signal to Noise ratio (PSNR) & Entropy. PSNR is higher than an existing method; BER & MSE of proposed method is less than an existing method.

Implementation

The proposed work has been implemented in MATLAB software using image processing and Wavelet toolbox. The compressed image is reconstructed into an original image by applying the inverse process.

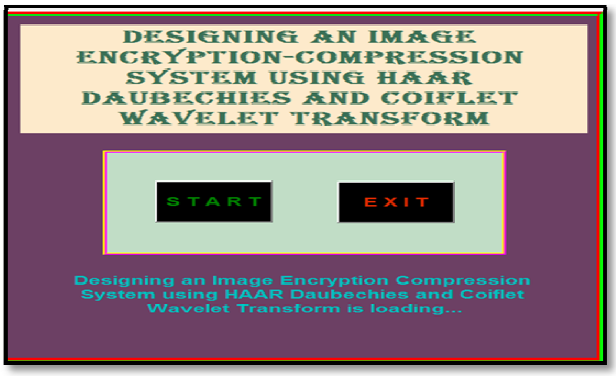

Figure.8: Home Page

Figure8 represents the home page for an image encryption and compression system. It consists of start or exit buttons for the user application.

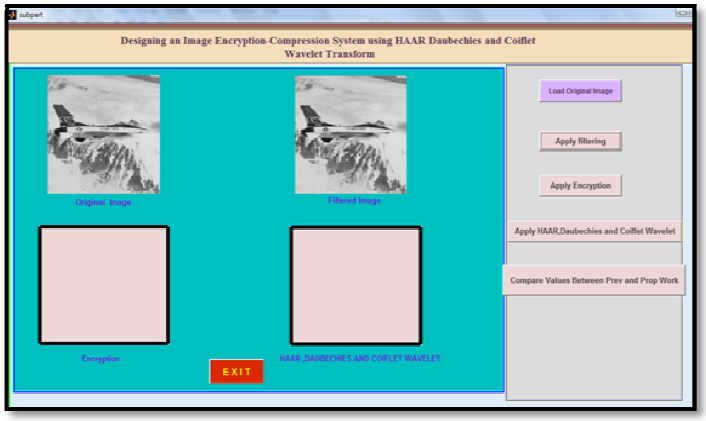

Figure.9: Loading of Image & Apply Filtering

Figure 9: represents loading of an image and filtering is applied to remove the noise.

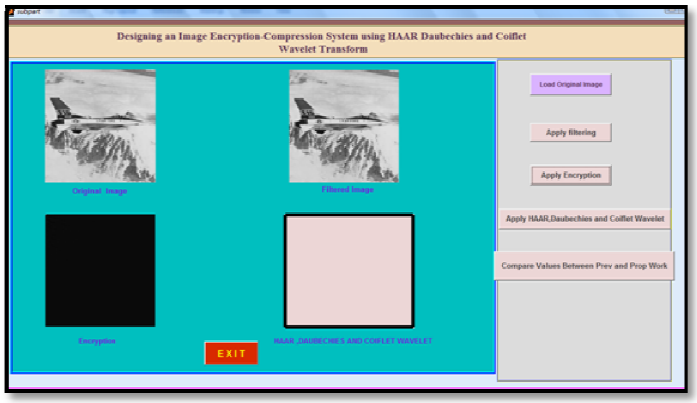

Figure.10: Apply Encryption

Figure.10: represents encryption to the filterd image using random permutation method.

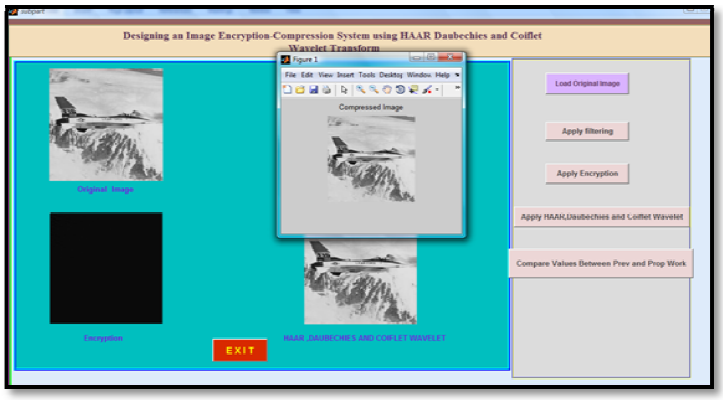

Figure.11: Apply Haar, Daubechies and Coiflet Wavelets

The compressed image after applying the Haar, Daubechies and Coiflet wavelet techniques is represented in figure.11. The pop up window shows a compressed image.

RESULTS AND DISCUSSIONS

The proposed work is analyzed by using various parameters like CR (Compression Ratio), MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio), BER (Bit Error Rate) and Entropy [15].

Compression Ratio (CR): It refers to ratio of the size of an original image to the size of compressed image.

$$C_R = \frac{n1}{n2}$$ *where n1 is the size of original image and n2 is the size of compressed image.*

MSE (Mean Square Error): MSE measures average of the square of the errors i.e. the cumulative squared error between the compressed and original image. A lower value of MSE shows less error.

$$MSE = \frac{\sum(f(i,j) - F(i,j))^2}{MN}$$

$f(i,j)$ is the original image, $F(i,j)$is the compressed image and MN is the size of image

PSNR (Peak Signal to Noise Ratio):It is most commonly used to measure the quality of reconstruction e.g. for image compression. The signal in this case is the original data, and the noise is the error introduced by compression. A higher PSNR indicates that the reconstruction is of higher quality

$$PSNR = 10 \log_{10} \left(\frac{255}{\sqrt{MSE}}\right)^2$$

Bit Error Rate(BER): BER is used in assessing systems that transmit digital data from one location to another. It is the ratio of the number of bit errors divided by the total number of transferred bits during a studied time interval. BER is a unitless performance measure, often expressed as a percentage

$$BER = \frac{\text{Number of Errors}}{\text{Total number of Bits Sent}}$$

Entropy: It is a statistical measure of randomness that can be used to characterize the texture of the input image. It is an important factor to estimate whether the digital image is basically the same with the original image. Usually, the higher the resolution is,the more similar the digital image to the original one. It is calculated with the help of in-built functions in MATLAB.

Table 2: Proposed Values of CR, MSE, PSNR, BER and Entropy

No	Image (JPEG) (512x512) pixels	CR	MSE	PSNR	BER	ENTROPY
1	BARBARA	1.1150	2.0615	52.7816	2.4145	7.6175
2	LENA	1.1492	1.6636	52.4059	2.4217	8.3760
3	BOAT	0.8344	1.0119	51.9253	2.4264	7.1171
4	PEPPERS	1.1254	1.4391	51.296	3.4157	8.5578
5	GOLD HILL	0.9969	2.5328	52.1992	2.4238	7.7733
6	AIRPLANE	0.8873	1.6298	52.8120	1.3482	7.5026
7	BRIDGE	1.3168	2.2629	52.6741	3.4147	8.4808
8	HARBOR	0.8346	2.6572	52.6678	2.3825	7.9666
9	MAN	1.1541	2.0809	52.5670	2.4150	7.4261
10	TANK	0.7722	1.1954	52.1396	2.4225	6.5135

Table 3: Comparison of PSNR and BER for Existing Method & Proposed Method

S. No.	Image (JPEG) (512x512) Pixels	PSNR of (Existing Method)	PSNR (Proposed Method)	BER (Existing System)	BER (Proposed System)
1	BARBARA	49.89	52.7816	3.074	2.4145
2	LENA	49.89	52.4059	2.588	2.4217
3	BOAT	49.90	51.9253	2.626	2.4264
4	PEPPERS	49.89	51.296	3.074	3.4157
5	GOLD HILL	49.89	52.1992	3.074	2.4238
6	AIRPLANE	49.91	52.8120	2.302	1.3482
7	BRIDGE	49.91	52.6741	3.890	3.4147
8	HARBOR	49.90	52.6678	3.366	2.3825
9	MAN	49.91	52.5670	2.850	2.4150
10	TANK	49.90	52.1396	3.164	2.4225

PSNR values in the case of proposed method is more than PSNR of an existing method and BER of proposed method is less than the BER of an existing method as shown in table 3.i.e. proposed method gives better results as compared to existing method.

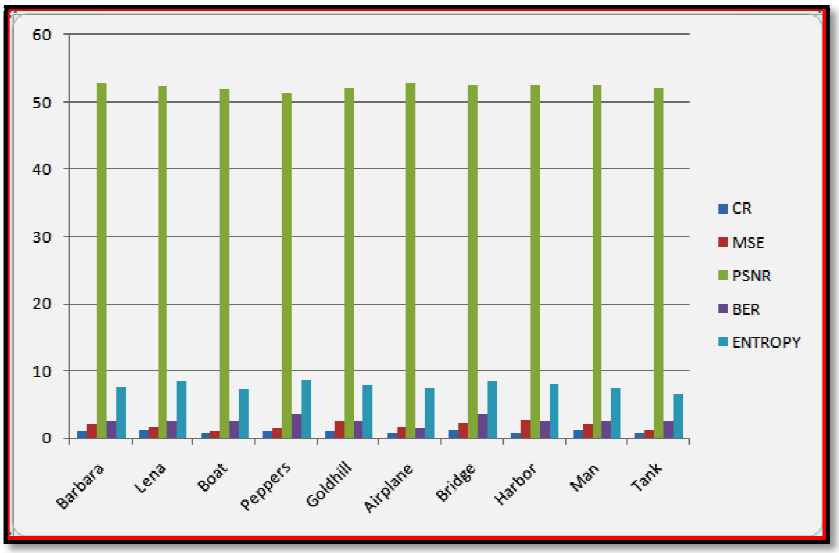

Figure 12: Proposed Values of CR, MSE, PSNR, BER & Entropy

CONCLUSION AND FUTURE SCOPE

In this paper, an efficient image encryption and compression system is designed using image transformation. An image encryption is achieved via random permutation. Compression of encrypted image is realized by using Haar, Daubechies and coiflet wavelet transform. Many Image Compression techniques have been proposed earlier but they were not secure enough and compression ratio is also poor. Image compression results was not better with daubechies wavelet. Thus, Haar wavelet is used in combination with Daubechies and coiflet wavelets for data compression. The results demonstrate that for test images, the loss of information is less hence the quality is better.In future, the technique can be extended by applying different transforms on colour image. High performance compression algorithms may be developed and implemented using neural networks and soft computing.

REFERENCES

1. Subramanya, S.R.,"*Image compression technique*", IEEE, Vol. 20, Issue 1, pp.19-23,Feb-March 2001.
2. Gonzalez, Rafael C., "*Digital image processing*. Pearson Education India, 2009.
3. Woods, R. C. 2008. "*Digital Image processing*" Pearson Prentice Hall, Third Edition
4. Komal D Patel, Sonal Belan,*"Image Encryption Using Different Techniques"*, International Journal of Emerging Technology and Advanced Engineering , Volume 1, Issue 1, November 2011,pp.30-34.
5. Rajinder Kaur,Er.Kanwalprit Singh,"*Image Encryption Techniques:A Selected Review"*, IOSR Journal of Computer Engineering (IOSR-JCE), Volume 9, Issue 6 (Mar-Apr. 2013), pp.80-83.
6. Prabhakar Telagarapu,V.Jagan Naveen,A.Lakshmi..Prasanthi , G.Vijaya Santhi, "*Image Compression Using DCT and Wavelet Transformations"*, International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol. 4,No. 3,September, 2011,pp.61-74.
7. S. Deva Simha, Mr.K.Mallikarjuna,*"Enhancement of Image Security Using Random Permutation"*, International Journal of Engineering Trends and Technology,Vol.17, No.8, pp.411-414, Nov 2014.
8. Marvel, Lisa M., and George W. Hartwig Jr. ,"*A Survey of Image Compression Techniques and their Performance in Noisy Environments*",No. ARL-TR-1380, Army Research Lab Aberdeen Proving Ground Md,1997,
9. R. Lazzeretti and M. Barni, "*Lossless compression of encrypted grey- level and color images*," proceedings of 16th European Signal Processing Conference, Aug. 2008, pp. 1–5.
10. Gleb v. Tcheslavski ,"*Basic Image Compression Methods*", springer in 2008 ELEN 4304/5365 DIP.
11. Piotr Porwik, Agnieszka Lisowsk, "*The Haar–Wavelet Transform in Digital Image Processing: Its Status and Achievements"*, Machine Graphics and Vision, vol. 13, issue 1/2, 2004.
12. Ms. Sonam Malik and Mr. Vikram Verma,"*Comparative analysis of DCT, Haar and Daubechies Wavelet for Image Compression*", International Journal of Applied Engineering Research,Vol.7 No.11,2012.
13. Sandeep kaur, Gaganpreet Kaur, Dr.Dheerendra Singh,"*Comparative Analysis Of Haar And Coiflet Wavelets Using Discrete Wavelet Transform In Digital Image Compression*", International Journal of Engineering Research and Applications (IJERA), Vol. 3, Issue 3, May-Jun 2013, pp.669-673.
14. Jiantao Zhou, Xianming Liu, Yuan Yan Tang," *Designing an Efficient Image Encryption-Then Compression System via Prediction Error Clustering and Random Permutation"*, Information Forensics and Security, IEEE Transactions,Vol9 , Issue 1,pp.39-50,2014
15. Vinay U. Kale & Nikkoo N. Khalsa," *performance Evaluation of Various Wavelets for Image Compression of Natural and Artificial Images*", International Journal of Computer Science & Communication, Vol. 1, No. 1, January-June 2010, pp. 179-184.
16. D. Klinc, C. Hazay, A. Jagmohan, H. Krawczyk, and T. Rabin, "*On compression of data encrypted with block ciphers*," IEEE Transactions on Information Theory, vol. 58, no. 11, pp. 6989–7001, Nov. 2012.